AO-106 (Rev: 06/09)-Application for Search Warrant

FILED

MAR 14 2024

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
a Samsung Galaxy S21 FE 5G, serial number R5CTA17BEDM, and IMEI 351844421422359, Currently Stored at Homeland Security Investigations Tulsa Office

Case No. 24-MJ-159-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)	Possession of and Access with Intent to View Child Pornography

The application is based on these facts:

See Affidavit of SA Dustin Carder, HSI, attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Dustin Carder, Special Agent, HSI
Printed name and title

Subscribed and sworn to by phone.

Date: 3/14/24

Judge's signature

City and state: Tulsa, Oklahoma

Jodi F. Jayne, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of a Samsung Galaxy S21 FE 5G, serial number R5CTA17BEDM, and IMEI 351844421422359, Currently Stored at Homeland Security Investigations Tulsa Office	**Case No. _____**

Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize

I, Dustin L. Carder, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") since December 2018. I am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to

investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's (FLETC) twelve-week Criminal Investigator Training Program (CITP) and the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252(a).

4. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) will be

located in the electronically stored information described in Attachment B and is recorded on the Device described in Attachment A.

Jurisdiction

6. "[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a.

7. The requested search is related to the following violations of federal law:

> a. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. Venue is proper because the person or property described in this affidavit is located within the Northern District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

Identification of the Device to be Examined

9. The property to be searched is a Samsung Galaxy S21 FE 5G, serial number R5CTA17BEDM, and IMEI 351844421422359, hereinafter the "Device." The Device is currently located at Homeland Security Investigations, 125 West 15th Street, Suite 500, Tulsa, Oklahoma 74119.

10. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Definitions

11. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means

the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet;

c. "Electronic Mail," commonly referred to as email (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Email systems are based on a store-and-forward model; that is, email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an email server, for as long a period of time as it takes to send or receive messages. One of the most commons methods of obtaining an email account is through a free web-based email service provider such as, Outlook, Yahoo, or Gmail. Anyone with access to the Internet can generally obtain a free web-based email account;

d. A "hash value" or "hash ID" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names;

e. "Cloud storage service" refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

f. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state;

g. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;

h. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form;

i. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b)

bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and

j. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Background of NCMEC and the CyberTipline Program

12. The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further the mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Program. NCMEC makes information submitted to the CyberTipline and Child Victim Identification Program available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers (ESPs), law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC performs its programs of work pursuant to its own private mission and independent business

operations. NCMEC does not act in the capacity of or under the direction or control of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.

13. NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and ESPs can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sex abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. CyberTipline Reports (CyberTips) are distributed by NCMEC analysts to law enforcement agencies who may have legal jurisdiction in the place that victims and suspects are believed to be located based on information provided in the CyberTips.

Probable Cause

14. In October 2023, HSI Tulsa received information from the Tulsa County Sheriff's Office ("TCSO") regarding Bryon Alan LEE, a U.S. citizen and previously convicted sex offender. Multiple CyberTips from NCMEC had been generated regarding Google account "bryonalee1992@gmail.com" from Imgur, LLC[1],

[1] Imgur, LLC is an online content hosting site where users can view and share content such as images, GIFs, memes, videos, and reviews. Users can communicate with other users by posting public comments or sending private messages, GIFs, or emojis. Imgur is available on web browser and mobile application.

Dropbox, Inc.[2], and Discord[3] due to the uploading of numerous images of child pornography to their platforms. These leads span between August 2019 and August 2023. LEE is an enrolled member of the Cherokee Nation tribe and resides in Sapulpa, Oklahoma, within the territorial boundaries of the Muscogee Creek Nation, in the Northern District of Oklahoma.

15. On October 30, 2023, TCSO Detective Matt Gray was assigned four (4) CyberTips from NCMEC. The four CyberTips had email address "bryonalee1992@gmail.com" in common and spanned from 2019 to 2023. After an initial investigation, Gray determined that the suspect, Bryon LEE, was Native American and resided outside of his jurisdiction in Sapulpa, Oklahoma. Gray then sought my assistance in the investigation. The CyberTips will be detailed in the following paragraphs.

CyberTip 65655420

16. CyberTip 65655420 was reported by Imgur, LLC on March 9, 2020. Imgur reported that on August 7, 2019, a user with email address "bryonalee1992@gmail.com" uploaded 108 images to their platform that were flagged. Five IP addresses were associated with the uploads: two were Verizon Wireless, two were Cox Communications, and one was AT&T Wireless. The two

[2] Dropbox is a file hosting service operated by the American company Dropbox, Inc., headquartered in San Francisco, California, U.S. that offers cloud storage, file synchronization, personal cloud, and client software.

[3] Discord is an instant messaging and VoIP social platform. Users have the ability to communicate with voice calls, video calls, text messaging, media, and files in private chats or as part of communities called "servers."

Cox Communications IP addresses geolocated to Edmond, Oklahoma. It was later determined that LEE resided in Edmond, Oklahoma during this time.

17. According to the CyberTip, as it pertains to them viewing the image or if they were publicly available, for each image it reads "Information Not Provided by Company." NCMEC reported that 13 of the files were automatically categorized based on their review of the uploaded files OR a "hash match" of one or more uploaded files to visually similar files that were previously viewed and categorized by NCMEC at the time the report was generated. Five of these 13 files were categorized as "CP (Unconfirmed)." I reviewed the images and observed them to consist of multiple prepubescent female victims topless, with bare chest exposed; multiple computer-generated media files depicting pornography; adult pornography; age-difficult females who are nude; and clothed prepubescent female victims posed in a provocative manner and/or wearing inappropriate clothing.

CyberTip 65654483

18. CyberTip 65654483 was reported by Imgur, LLC on March 9, 2020. Imgur reported that on November 25, 2019, a user with email address "bryonalee1992@gmail.com" uploaded 70 images to their platform that were flagged. The IP address used was 68.97.86.119, which geolocated to Edmond, Oklahoma, and was serviced by Cox Communications.

19. According to the CyberTip, as it pertains to them viewing the image or if they were publicly available, for each image it reads "Information Not Provided by Company." NCMEC reported that three of the files were automatically categorized

based on their review of the uploaded files OR a "hash match" of one or more uploaded files to visually similar files that were previously viewed and categorized by NCMEC at the time the report was generated. One of the files was categorized as "Child Clothed," and the other two as "Child Unclothed."

20. Imgur stated that any image constituting child abuse sex imagery (CSAI) is flagged on their system in one of four ways:

a. We use software that proactively compares new uploads to known CSAI hashes. If there's a match, the image and its associated information are automatically sent to NCMEC.
b. NCMEC sends us a daily list of items to report and delete; we copy and paste the list and proceed in the same way as mentioned above.
c. Our users are very quick to report any abuses they see; moderators view all such reports quickly and report any CSAI to NCMEC.
d. On occasion, Imgur employees themselves come across CSAI in the course of their work, and again it's reported to NCMEC. We do not track the method by which CSAI images happen to be found, nor do we maintain any records of which Imgur employees (if any) may have seen them. All images on Imgur are publicy accessible via their direct image links.

21. Due to the factors mentioned above, I viewed each image associated with the CyberTip. I observed many of the same images that were flagged in the previous CyberTip, which depicted prepubescent minor females posing in a provocative manner and/or wearing inappropriate clothing.

22. In April 2020, an Oklahoma State Bureau of Investigation (OSBI) analyst searched TLO[4] for email address "bryonalee1992@gmail.com." The email address

[4] TransUnion's TLO is an online investigative database utilized by law enforcement containing personal information, including peoples' physical addresses, phone numbers, email addresses, and the contact details of possible relatives.

was found to be linked to Bryon LEE, date of birth XX/XX/1992, at an apartment in Edmond, Oklahoma. Bryon LEE's name is fully listed in the suspect email address, as well as his birth year: 1992.

CyberTip 84142079

23. CyberTip 84142079 was reported by Dropbox on January 6, 2021. Dropbox reported that on January 5, 2021, at 01:10:42, a user with email address "bryonalee1992@gmail.com," username "Bryon Lee," with User ID number 3364911424, uploaded an image file to their platform that was flagged. The image with filename "Photo Jul 26, 11 00 58 PM.png" and MD5 value 40367f16f63a443c01823e845f1266b5 was categorized as "Apparent Child Pornography." This image was publicly available and was also viewed by one or more Dropbox employees. As such, I viewed the image. It is described as a nude prepubescent white female with no breast development and no pubic hair. The minor victim (MV) appears to be under the age of 12. MV is bound by her hands and feet to a mirror using suction cups connected to binding straps. MV's vagina is visible in the image. This image meets the federal definition of child pornography, as stated in Title 18, United States Code, Section 2256.

CyberTip 170916680

24. CyberTip 170916680 was reported by Discord on August 16, 2023. Discord reported that on August 16, 2023, at 00:58:32 UTC, username "dracusdemonica#0" with User ID number 246423663790915585 uploaded one image to their platform that was flagged. The image with filename "user23476379_f5a935dec2ec.jpg" with

MD5 value fba226d428a8a43f456b5f733991bd05 was viewed by one or more Discord employees, was publicly available, and classified as "Apparent Child Pornography." As such, I viewed the image. It is described as two minor female victims, one who is clothed, and the other who appears to be nude. The nude victim has little breast development. Both minor victims have their hands on the erect penis of an unknown male. The image meets the federal definition of child pornography, as stated in Title 18, United States Code, Section 2256.

25. Discord also provided verified phone number (918) 982-5823, and verified email address "bryonalee1992@gmail.com" that are associated with the account. The IP address utilized by the account during the upload was 98.178.189.190, which is serviced by Cox Communications and geolocates to Sapulpa, Oklahoma.

26. TCSO Detective Gray queried phone number (918) 982-5823 in Thomson Reuters' CLEAR[5]. Gray discovered the phone number was associated with Bryon LEE at 710 West Teel Road in Sapulpa, Oklahoma. This falls within the Muscogee Creek Nation in the Northern District of Oklahoma.

Previous Sex Offense Involving Bryon Lee

27. In conducting this investigation, I learned that LEE is a registered sex offender for a 2020 Edmond Police Department case where LEE was convicted of Using Technology to Engage in Sexual Communication with a Minor (Oklahoma County CF-2021-1236). LEE received a 10-year suspended sentenced and was to be

[5] CLEAR is a powerful research tool that assists law enforcement by combining billions of public records, to locate individuals, identify assets, and find key connections.

under the supervision of the Department of Corrections. This case involved LEE sending inappropriate and sexual communications and material via Facebook Messenger to a sixteen-year-old employee, his subordinate, at Taco Bell where he was the manager.

28. I learned that LEE is currently registered with the Muscogee Creek Nation Lighthorse Police (MCNLP). On October 31, 2023, I contacted the MCNLP and learned that his sex offender registration address is 710 West Teal Street, #24, Sapulpa, Oklahoma 74066. MCNLP advised that he registers every six months, and he last registered on July 18, 2023. MCNLP also had phone number (918) 982-5823 as his registered number, which is the same verified phone number connected to the Discord account described herein.

29. On November 3, 2023, HSI Tulsa electronically served Verizon Wireless with an administrative DHS summons for subscriber information for phone number (918) 982-5823 for a time frame of August 1, 2023, through the present.

30. On November 13, 2023, Verizon responded to the summons and provided the requested information. The number is registered to Bryon A. LEE with a contact address of 710 W. Teel Road, Trailer 24, Sapulpa, OK 74066. The account has been active since January 6, 2018. The email address associated with the Verizon account is bryonalee1992@gmail.com.

31. On November 15, 2023, I obtained federal search and seizure warrants in the Northern District of Oklahoma for the following: LEE's residence – 710 West Teel Road, Trailer 24, Sapulpa, OK 74066; LEE's vehicle – a red 2015 Chevrolet Spark

with Oklahoma license plate CHN-562, VIN KL8CF6S91FC74; and LEE's person. The warrants were authorized by U.S. Magistrate Judge Jodi F. Jayne.

32. On November 16, 2023, at approximately 0755 hours, HSI special agents, task force officers, the Sapulpa Police Department, and the Muscogee Creek Nation Lighthorse Police served the search warrants at LEE's residence. The marked Sapulpa Police unit activated their emergency lights and chirped the siren moments before HSI SA Jessica Jennings made multiple knock and announcements. LEE came to the front door and was escorted out of the residence before being placed into handcuffs.

33. Detective Matt Gray and I attempted to interview LEE in my vehicle. I showed LEE the search warrants, and explained what they were for. I advised LEE that he was not under arrest, but wanted to let him know what his rights were. LEE stated he did not want to speak without an attorney present. I then terminated the interview. As a result of the search warrants, multiple electronic devices, including LEE's cell phone, were seized at the scene, and later forensically examined.

Review of Dell Inspiron N5050 Laptop

34. I reviewed the data on a Dell Inspiron N5050 laptop computer (S/N: 823KJR1) seized during the search warrant. The owner of the device is listed as "Bryon," and the displayed computer name is "Bryon-PC." The laptop did have the CCleaner program. CCleaner, developed by Piriform Software, is a utility used to clean potentially unwanted files and invalid Windows Registry entries from a computer. CCleaner is often viewed as an anti-forensic tool due to its capabilities.

35. I located 26 files of child pornography on the device. Three are videos, and the remaining are images. There are five unique images of child pornography on the laptop; the remaining 18 are duplicates of those images.

36. One of the videos is twelve seconds long and depicts a prepubescent female victim in an outdoor setting. The victim's chest is exposed, and she has no visible breast development. There is a male masturbating with his penis positioned close to the victim's face. The male then ejaculates onto/into the face, hair, and mouth of the victim.

37. Another one of the videos is seven seconds long and depicts a prepubescent female victim wearing a purple shirt with a fairy or similar character on it. The female appears to be in the seated position. There is a male standing near the female with his penis exposed. The male appears to try and insert his penis into the victim's vagina. He then rubs his penis against her vagina. The victim is small in stature and had no visible pubic hair or development.

38. The remaining images and video depict prepubescent minor victims whose vaginas are displayed or are engaged in a sexual act.

Review of Samsung S21 FE Phone

39. I reviewed a Samsung S21 FE phone, IMEI: 350799511581772 seized during the search warrant. The Bluetooth name of this device is "Bryon's S21 FE." Multiple Chrome Autofill fields were also discovered for the name Bryon LEE, email address "bryonalee1992@gmail.com," and "DracusDemonica." I also located the usernames of "Oldddy4little," and "P3rvddy." I understand the first to mean that an older

person is interested in a younger person, and the second is a short-hand form of "Perv" or "Pervert daddy." I was not able to determine which websites or programs the usernames were related to.

40. Based on images located, it also appears that LEE took pictures of his six-year-old daughter's buttocks and pubic/groin region while she slept. The victim is wearing underwear in both images. Both images appear to have been taken on September 15, 2023, at 3:20 AM, while the victim was most likely asleep. The victim's face was not shown in either image. In both images, the victim is laying on a black sheet with repetitive diamond or flower-shaped designs on it. Another image located shows LEE's daughter, fully clothed, with her face shown, standing next to the bed with the same sheet on it.

41. LEE's daughter, M.L. was later forensically interviewed and disclosed that LEE took pictures of her body, and videos of her butt when she had no clothes on. M.L. was given an outline of a body on a child so she could show what she meant by "butt;" M.L. circled the buttocks of the female child on the provided image.

42. I also located 41 files of child pornography on the device, with 28 of those being visually unique. Four of the files are videos, while the remaining are images. Two of the videos depict minor female victims who undress and display their vaginas on camera. One of the videos depicts a young female who takes off her clothing and masturbates on camera. Her vagina is visible. She has slight budding of the breasts. The remaining video depicts a school-aged adolescent female performing oral sex on an adolescent male while another adolescent male is engaging is vaginal or anal sex

with her from behind. Most of the images depicts toddler-aged to approximately twelve-year-old female victims whose vaginas are displayed and/or are engaged in a sexual activity.

43. I located a partial Snapchat conversation between usernames "whiteboi2027512," and "randoma237722" while reviewing data on LEE's Samsung S21 phone. During this chat, an image of an 11-year-old female is shared, and the pair discuss the female in a sexually explicit manner. The below chat was located on LEE's phone.

Sender	**Recipient(s)**	**Message**	**Type**	**Message Date/Time - Central Time**
randoma237722	whiteboi2027512	Ye	Text	9/18/2023 8:42:39 PM
whiteboi2027512	randoma237722	I'd love to see her tiktok	Text	9/18/2023 8:44:28 PM
whiteboi2027512	randoma237722	Hey	Text	9/18/2023 8:39:45 PM
randoma237722	whiteboi2027512	Hi	Text	9/18/2023 8:39:49 PM
whiteboi2027512	randoma237722	Let's see her	Text	9/18/2023 8:40:06 PM
randoma237722	whiteboi2027512	She's 11	Text	9/18/2023 8:40:14 PM
whiteboi2027512	randoma237722	Ok	Text	9/18/2023 8:40:32 PM
randoma237722	whiteboi2027512	U wanna see	Text	9/18/2023 8:40:52 PM
randoma237722	whiteboi2027512		Call/Deleted message/Mini/Game	9/18/2023 8:40:57 PM
whiteboi2027512	randoma237722	Yes	Text	9/18/2023 8:41:22 PM
whiteboi2027512	randoma237722	Cutie	Text	9/18/2023 8:41:58 PM

randoma237 722	whiteboi202 7512	Will u trib her	Text	9/18/2023 8:42:49 PM
whiteboi202 7512	randoma237 722	Yes! Anymore?	Text	9/18/2023 8:43:35 PM
randoma237 722	whiteboi202 7512	Only that one pic it was from her tiktok	Text	9/18/2023 8:44:10 PM
whiteboi202 7512	randoma237 722	She's got me so hard	Text	9/18/2023 8:44:11 PM
randoma237 722	whiteboi202 7512	Ik sameeee	Text	9/18/2023 8:44:23 PM

44. I was not able to view any media associated with this conversation. I know from previous child exploitation investigations that when "randoma23722" is asking "whiteboi2027512" if he will "trib" to the image that he means masturbate to the image. "Trib" is short for "tribute" or "tribute material." In most cases, this means that the person receiving the image or video will masturbate to it, and then send an image or video to the sender of themselves in or completing the act of masturbation.

45. I was able to determine that the "whiteboi2027512" account was native to LEE's Samsung S21 FE 5G, IMEI: 350799511581772. The User ID associated with this Snapchat account is 7a087439-9cbf-4d51-8bec-3152b7eb3690, and the email address is "lewrachel747@gmail.com." This email address is also associated with a Discord account belonging to LEE.

Review of CyberPower PC Desktop

46. I reviewed the data on a CyberPower PC desktop computer, with product ID 00325-81628-12668-AAOEM seized during the search warrant. The owner is listed as "bryonalee1992@gmail.com." User "Bryon Lee" is listed as an administrator and

user. The program CCleaner was also located on this device, as well as Discord and peer-to-peer file sharing program "uTorrent."

47. I located 12 images of child pornography on the device, with seven of them being visually unique and the remainder duplicates. These files depict prepubescent females with their vaginas displayed and/or engaged in a sex act.

New Device Seized

48. On February 29, 2024, an arrest warrant was issued based on a criminal complaint for LEE for the following offenses: 18 U.S.C. §§ 2251(d)(1)(A) & 2251(e) – Notice or Advertisement Seeking Child Pornography; 18 U.S.C. §§ 2252(a)(2) and (b)(1) – Receipt and Distribution of Child Pornography; and 18 U.S.C. §§ 1151, 1153, and 2252(a)(4)(A) and (b)(2) – Possession of Child Pornography in Indian Country. The arrest warrant was granted by U.S. Magistrate Judge Susan E. Huntsman in the Northern District of Oklahoma.

49. I sought the assistance of the U.S. Marshal's Northern Oklahoma Violent Crimes Task Force (USMS-NOVCTF) in placing LEE into custody. The USMS-NOVCTF arrested LEE without incident on February 29, 2024, at his employer, Five Guys restaurant, at 9635 Riverside Parkway, Tulsa, Oklahoma, without incident.

50. When LEE was taken into custody, he had personal property, including a **Samsung Galaxy S21 FE 5G**, the **Device**. This property was left at LEE's employer after he was arrested. Audrey Steinberg, LEE's girlfriend, was at a nearby retail store when the arrest happened. I notified Georgia Steinberg, Audrey Steinberg's mother,

of the arrest so that she could assist Audrey in getting home, as Audrey does not drive. Georgia and Audrey retrieved LEE's personal property, including his phone, from LEE's employer.

51. On March 5, 2024, Georgia Steinberg informed me that she had looked at LEE's phone and found pornography and records indicating LEE had been sending money to girls. Georgia stated that she did not see any nude images of children, although some of the images she was not able to tell the age of the person. I advised Georgia to stop looking at the device and that I would take custody of the phone and seek a search warrant to view the contents.

52. On March 6, 2024, HSI Task Force Officer (TFO) Don Stach and I met with Georgia and Audrey Steinberg at their residence in Tulsa. Georgia turned over the device to me. The device was powered off. I asked if there was a passcode for the device, which Georgia provided as 0115. Audrey stated this was the birthdate of their daughter, M.L.

53. After transporting the device back to HSI Tulsa, I powered on the device, and went into Settings and the "About Phone" section to obtain the identifiers for the device for this search warrant. No other data on the device was reviewed or examined.

54. On the "About Phone" screen, SA Carder observed the phone number as 918-982-5823; product name as Galaxy S21 FE 5G; model name as SM-G990U2; serial number as R5CTA17BEDM; and IMEI as 351844421422359. The phone was then

secured in an HSI evidence bag and stored in the HSI Tulsa evidence room until this search warrant can be obtained.

55. Due to this investigation revealing that LEE had child pornography on multiple devices, and Georgia Steinberg observing age-difficult pornography and indications of money being sent to girls on the Device, it is likely that the Device contains child pornography, and/or other information involving the sexual exploitation of minors.

56. The Device is currently in the lawful possession of HSI. It came into HSI's possession in the following way: seized by HSI on March 6, 2024, pursuant to a report by Georgia Steinberg of age-difficult pornography and money being sent to girls observed on the Device.

57. The Device is currently in storage at Homeland Security Investigations, 125 West 15th Street, Suite 500, Tulsa, Oklahoma 74119, within the Northern District of Oklahoma. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

Technical Terms

58. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various

types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a

mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—

IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

59. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device.

Characteristics Common to Individuals who Exhibit a Sexual Interest in Children and Individuals who Distribute, Receive, Possess and/or Access with Intent to View Child Pornography

60. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children

engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through

the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"[6] it;

h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Background on Child Pornography, Computers, and the Internet

61. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

[6] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

a. Computers, smartphones[7] and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through

[7] Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone

with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases; and

g. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

62. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a

hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Electronic Storage and Forensic Analysis

63. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

64. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including possession, receipt, and distribution of child pornography. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

65. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Sessions" and

"GroupMe." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include possession, receipt, and distribution of child pornography.

66. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

67. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

68. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

69. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

70. *Methods of examination*. In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crimes under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data,

keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

71. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), has been violated, and that evidence of this offense, more fully described in Attachment B, are located on the Device described in Attachment A. I respectfully request that this Court issue a search warrant for the property described in Attachment A, authorizing the seizure of the items described in Attachment B.

72. Based upon my training and experience, I have learned that criminals who utilize the Internet actively search for criminal affidavits and search warrants and disseminate them to other criminals as they deem appropriate, i.e., post them publicly online through forums. It is possible that additional suspects will be discovered during forensic analysis of electronic devices. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting the potential target(s) to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

Dustin L. Carder
Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone on March 14th, 2024.

JODI F. JAYNE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched is a Samsung Galaxy S21 FE 5G, serial number R5CTA17BEDM, and IMEI 351844421422359, hereinafter the "Device." The Device is currently located at Homeland Security Investigations, 125 West 15th Street, Suite 500, Tulsa, Oklahoma 74119, in the Northern District of Oklahoma.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Device described in Attachment A that relate to violations of Title 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) involving Bryon LEE, including:

A. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found, including, but not limited to:

   i. Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) of child pornography; files relating to the distribution, receipt, or possession of child pornography, or information pertaining to an interest in child pornography;

ii. Files in any form containing the visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

iii. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors.

B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iii. Any and all electronic and/or digital records and/or documents pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;

iv. Any and all electronic and/or digital records and/or documents including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;

v. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums;

vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software.

C. Records or other items which evidence ownership, use, or control of the Device described in Attachment A.

D. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access.

E. Any and all information, correspondence (including emails), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educing, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.